

10/669,269 10/06/05
(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
19. Juli 2001 (19.07.2001)

PCT

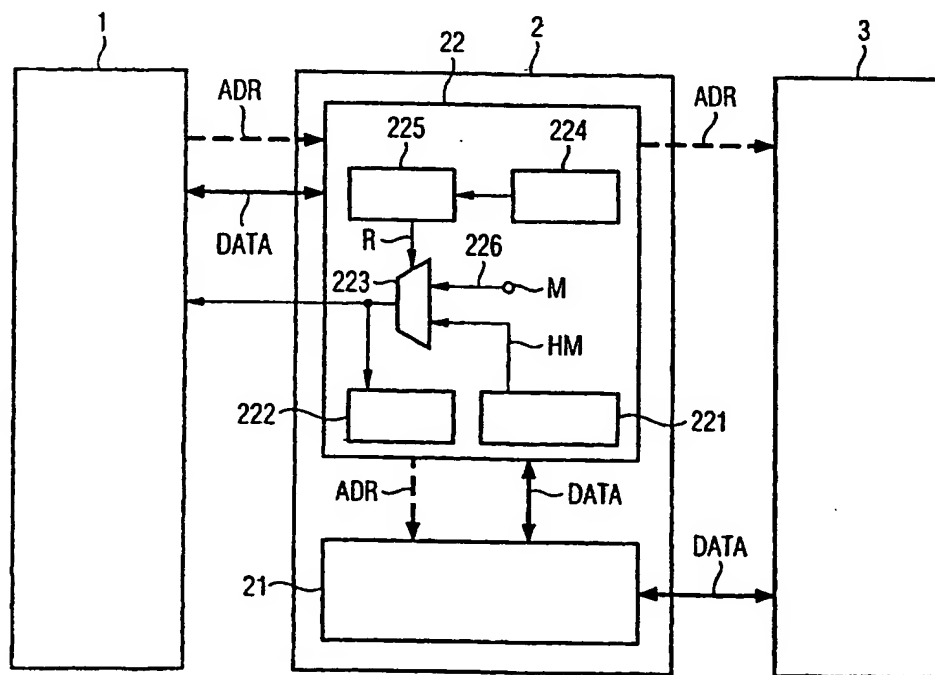
(10) Internationale Veröffentlichungsnummer
WO 01/52069 A2

- (51) Internationale Patentklassifikation⁷: G06F 12/08 (72) Erfinder; und
(21) Internationales Aktenzeichen: PCT/EP00/13134 (75) Erfinder/Anmelder (nur für US): GAMMEL, Berndt
[DE/DE]; Ludwig-Dill-Weg 3, 81737 München (DE).
(22) Internationales Anmeldedatum: SMOLA, Michael [DE/DE]; Juttastrasse 17, 80636
22. Dezember 2000 (22.12.2000) München (DE).
(25) Einreichungssprache: Deutsch (74) Anwalt: EPPING HERMANN & FISCHER; Postfach
12 10 26, 80034 München (DE).
(26) Veröffentlichungssprache: Deutsch
(30) Angaben zur Priorität: (81) Bestimmungsstaaten (national): BR, CN, IN, JP, KR,
00100508.1 11. Januar 2000 (11.01.2000) EP MX, RU, UA, US.
(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von (84) Bestimmungsstaaten (regional): europäisches Patent (AT,
US): INFINEON TECHNOLOGIES AG [DE/DE]; St.- BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
Martin-Strasse 53, 81669 München (DE). NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: MEMORY ACCESS METHOD AND A CIRCUIT ARRANGEMENT

(54) Bezeichnung: SPEICHERZUGRIFFSVERFAHREN UND SCHALTUNGSANORDNUNG



(57) Abstract: The invention relates to a microprocessor (1). A cache memory (21) serves for accelerating access to an external memory (3). Cache miss is signalled to the microprocessor (1) instead of the actually present cache hit event. Reversal is controlled randomly. The current profile of cache hit and cache miss events is thus masked in such a way that security is increased in relation to statistic hacking methods by means of which the current profile is evaluated.

[Fortsetzung auf der nächsten Seite]

WO 01/52069 A2

**Veröffentlicht:**

- ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Bei einem Mikroprozessor (1) dient ein Cache-Speicher (21) zur Beschleunigung von Zugriffen auf einen externen Speicher (3). Anstelle eines tatsächlich vorliegenden Cache-Hit-Ereignisses wird dem Mikroprozessor (1) ein Cache-Miss gemeldet. Die Umsteuerung erfolgt zufallsgesteuert. Dadurch wird das Stromprofil von Cache-Hit- und Cache-Miss-Ereignissen verschleiert, so dass die Sicherheit gegenüber statistischen das Stromprofil auswertenden Angriffsverfahren erhöht wird.

Beschreibung

Speicherzugriffsverfahren und Schaltungsanordnung

5 Die Erfindung betrifft ein Verfahren zum Zugriff eines Mikro-
prozessors auf einen Speicher, bei dem ein Cache-Speicher
vorgesehen ist, in dem Teile des Inhaltes des Speichers zwi-
schenspeicherbar sind, bei dem der Mikroprozessor einen ge-
speicherten Datenwert anfordert, bei dem festgestellt wird,
10 ob der angeforderte gespeicherte Datenwert im Cache-Speicher
enthalten ist, und bei dem dann, wenn der Datenwert im Cache-
Speicher nicht enthalten ist, der Datenwert aus dem Speicher
ausgelesen wird, und bei dem ein Steuersignal erzeugt wird,
das dann, wenn der Datenwert im Cache-Speicher enthalten ist,
15 in Abhängigkeit des Steuersignals den Datenwert entweder aus
dem Cache-Speicher oder aus dem Speicher ausliest.

Die Erfindung betrifft außerdem eine Schaltungsanordnung zur
Durchführung eines solchen Verfahrens.

20

Mikroprozessorsysteme benötigen einen Speicher, um dauerhaft
oder flüchtig zu verarbeitende Daten oder Programme abzuspei-
chern. Bei der Abarbeitung des Programms greift der Mikropro-
zessor auf den Speicher zu, um aktuell benötigte Programmtei-
25 le oder Daten zu laden. Meist ist der Speicher in einem inte-
grierten Halbleiterchip als separater, externer Schaltungs-
block neben dem Mikroprozessor angeordnet. Zugriffe auf den
externen Speicher sind daher relativ langsam.

30 Zur Beschleunigung von Speicherzugriffen werden sogenannte
Cache-Speicher verwendet. Sie dienen dazu, die Latenzzeiten
bei Zugriffen auf die externen Speicher zu vermeiden, indem
oft benötigte Daten oder Instruktionen im Cache-Speicher zwi-
schengespeichert werden. Die Cache-Speicher sind gegenüber
35 den externen Speichern klein und schaltungstechnisch so aus-
geführt, daß sie auf eine Anfrage schnell antworten. Cache-
Speicher können zusammen mit dem Mikroprozessor auf dem glei-

chen Halbleiterchip integriert werden. Es werden sowohl Lese- als auch Schreibzugriffe über den Cache-Speicher abgewickelt werden.

- 5 Eine Leseanfrage des Mikroprozessors an den Speicher unter Verwendung von externem Speicher und Cache-Speicher läuft wie folgt ab. Zuerst wird überprüft, ob das angefragte Datum im Cache-Speicher enthalten ist. Wenn festgestellt wird, daß das Datum nicht im Cache-Speicher zwischengespeichert ist, sogenannte Cache-Miss, wird das Datum aus dem langsameren externen Speicher in den Cache-Speicher nachgeladen und dabei außerdem an den Mikroprozessor bereitgestellt. Wenn das angeforderte Datum im Cache-Speicher enthalten ist, sogenannter Cache-Hit, wird es sofort an den Mikroprozessor ausgelesen und von diesem verarbeitet.

Mikroprozessoren finden unter anderem Anwendung in sicherheitskritischen Systemen, beispielsweise in Chipkarten. Der Mikroprozessor wird dort unter anderem verwendet, um den Datenverkehr zwischen der Chipkarte und einem Lesegerät zu verschlüsseln, so daß ausreichend Sicherheit vor betrügerischen Angriffen zum Ausspähen der geheimen Informationen gewährleistet ist. Eine Angriffsart besteht darin, die Charakteristik des Stromverbrauchs des Mikroprozessors zu messen. Aus dem charakteristischen Stromprofil können Rückschlüsse auf den Programmablauf gezogen werden. Cache-Miss- und Cache-Hit-Ereignisse sind anhand des Stromprofils genau zu erkennen. Daraus könnten Rückschlüsse auf den verwendeten Ver- und Entschlüsselungsalgorithmus aufgrund der Anzahl und Lage der verwendeten Speicherzugriffe gezogen werden; es wäre dann möglich, weitere Rückschlüsse auf den speziellen Programmablauf zu ziehen, und anhand der Stromprofile Triggerpunkte zu erhalten, auf denen andere Meßverfahren aufsetzen.

- 35 Das jeweilige Stromprofil für Cache-Hit und Cache-Miss ist unterschiedlich. Während bei einem Cache-Hit sofort Daten aus dem Cache-Speicher zum Mikroprozessor ausgelesen werden, dau-

ert es bei einem Cache-Miss einige Zeit, bis der Cache-Speicher aus dem externen Speicher nachgeladen wird. Während der Anfangsphase ist daher der Stromverbrauch bei einem Cache-Miss niedriger als bei einem Cache-Hit. Während des
5 Nachladens des Cache-Speichers bei einem Cache-Miss erhöht sich dann der Stromverbrauch aufgrund der Vielzahl der Schaltvorgänge im Chip während des Nachladevorgangs. Der Stromverbrauch ist über die externen Anschlußpins der integrierten Schaltung oder der Stromzuführungsanschlüsse der
10 Chipkarte meßbar.

Ein Datenzugriff mit einem Cache-Miss dauert also relativ lange, und der Nachladevorgang bewirkt einen relativ hohen Stromverbrauch der Zentraleinheit des Mikroprozessors. Cache-
15 Hit- und Cache-Miss-Ereignisse führen dazu, daß die Zentraleinheit verschieden lange auf die Bereitstellung der Daten zu warten hat. Der Wartevorgang hat einen charakteristisch niedrigen Stromverbrauch der Zentraleinheit. Insgesamt liegt der Stromverbrauch bei einem Cache-Miss höher als bei
20 einem Cache-Hit. Mittels statistischer Auswerteverfahren unter Anwendung von Korrelationen auf das Aktivitätsmuster des Stromprofils können daraus Rückschlüsse auf die Verarbeitungsschritte innerhalb des Mikroprozessors und die verarbeiteten Daten gewonnen werden. Die Anwendung eines solchen her-
25 kömmlichen Mikroprozessors in sicherheitsrelevanten, geheime Informationen verarbeitenden Systemen ist daher problematisch.

In der US 5 765 164 ist ein Cache-Speicher beschrieben, bei
30 dem trotz eines Cache-Hit ein Cache-Miss signalisiert wird. Dadurch werden mögliche Zugriffskollisionen auf den Cache-Speicher vermieden. Eine deterministische Steuerung schaltet bei einem Cache-Hit auf einen Cache-Miss um.

35 In der US 4 932 053 ist ein zufallsgesteuerter Zugriff auf Dummy-Speicherzellen beschreiben, um das Stromprofil zu ver-

schleiern. Die US 5 500 601 bezieht sich allgemein auf das Problem der Abhörbarkeit des Stromprofils.

Die Aufgabe der Erfindung besteht darin, ein Verfahren für
5 einen Zugriff eines Mikroprozessors auf einen Speicher unter Anwendung eines Cache-Speichers anzugeben, welches eine höhere Abhörsicherheit bietet.

Eine weitere Aufgabe besteht darin, eine Schaltungsanordnung
10 anzugeben, die eine höhere Abhörsicherheit gewährt..

Gemäß der Erfindung wird die Aufgabe betreffend das Verfahren durch ein Verfahren gelöst zum Zugriff eines Mikroprozessors auf einen Speicher, bei dem ein Cache-Speicher vorgesehen
15 ist, in dem Teile des Inhaltes des Speichers zwischenspeicherbar sind, bei dem der Mikroprozessor einen gespeicherten Datenwert anfordert, bei dem festgestellt wird, ob der angeforderte gespeicherte Datenwert im Cache-Speicher enthalten ist, und bei dem dann, wenn der Datenwert im Cache-Speicher
20 nicht enthalten ist, der Datenwert aus dem Speicher ausgelesen wird, wobei ein Steuersignal erzeugt wird, das dann, wenn der Datenwert im Cache-Speicher enthalten ist, in Abhängigkeit des Steuersignals den Datenwert entweder aus dem Cache-Speicher oder aus dem Speicher ausliest, wobei das Steuersi-
25 gnal in zufallsgesteuerter Weise erzeugt wird.

Betreffend die Schaltungsanordnung wird die Aufgabe durch eine Schaltungsanordnung gelöst, die umfaßt: eine zentrale Verarbeitungseinheit, einen Speicher, einen Cache-Speicher und
30 eine Steuerungseinrichtung, die mit der zentralen Verarbeitungseinheit und dem Cache-Speicher verbunden ist, wobei die Steuerungseinrichtung enthält: einen Zufallsgenerator zur Erzeugung eines zufallsgesteuerten Signals, eine Einrichtung zur Feststellung, ob ein von der zentralen Verarbeitungseinheit angefragter Datenwert im Cache-Speicher enthalten ist
35 oder nicht, einen Anschluß zur Bereitstellung eines Signals, das angibt, daß der Datenwert nicht im Cache-Speicher enthal-

ten ist, und eine Umschalteneinrichtung, die vom Zufallsgenerator steuerbar ist, und die eingangsseitig mit dem Anschluß und der Einrichtung zur Feststellung verbunden ist, und ausgangssseitig mit der zentralen Verarbeitungseinheit gekoppelt ist, um ein Auslesen entweder aus dem Speicher oder aus dem Cache-Speicher in Abhängigkeit von einem an der Umschalteneinrichtung ausgangssseitig anliegenden Signal steuerbar ist.

Es können einer oder mehrere Cache-Speicher vorhanden sein.

Die beschriebene Schaltungsanordnung und das Verfahren können zweckmäßigerweise für alle Cache-Speicher angewandt werden.

Die genannte Steuereinrichtung kann entweder zentral für alle Cache-Speicher gemeinsam verwendet werden oder mehrfach vorhanden sein und einzelnen Cache-Speichern individuell zugeordnet werden. Es sind Cache-Speicher für zu verarbeitende Daten und Cache-Speicher für Instruktionen als auch Cache-Speicher für Daten und Instruktionen gemeinsam bekannt, sogenannte "Unified Caches". Der Begriff "Datenwert" umfaßt sowohl zu verarbeitende Daten als auch Instruktionen.

20

Bei dem erfindungsgemäßen Verfahren bzw. der Schaltungsanordnung wird die Korrelation von Stromsignaturen, die bei Cache-Hits und Cache-Misses auftreten, zum Programmablauf verschleiert. Die Erfindung sieht hierzu ein Steuersignal vor,

25 durch welches ein zusätzlicher Eingriff in die Speicherzugriffssteuerung möglich ist. Dadurch kann dann, wenn ein Cache-Hit festgestellt wird, trotzdem der Speicherzugriff in Form eines Cache-Miss abgewickelt werden. Praktischerweise werden Cache-Hits in geeigneter Weise durch Cache-Misses ersetzt. In die Cache-Steuerungslogik wird neben deren Abhängigkeit vom Cache-Inhalt und der Zugriffsadresse außerdem mittels des Steuersignals eingegriffen, um Cache-Misses zusätzlich einzufügen. Das Steuersignal wird durch andere Parameter als die Trefferquote bei Cache-Hits gesteuert. Dadurch wird erreicht, daß das von außen meßbare Stromprofil des Mikroprozessors und die Abfolge von Cache-Misses und Cache-Hits nicht mehr mit dem Programmablauf übereinstimmen. Ein Rück-

schließen auf den Programmablauf durch Messung des Stromprofils wird daher wesentlich erschwert.

Das Steuersignal wird unter Anwendung von Zufallsmustern erzeugt. Die Erzeugung von Zufallsmustern ist hinreichend bekannt. Hierzu eignen sich Zahlenfolgen, die so erzeugt werden, daß sie physikalisch zufällig oder pseudo-zufällig sind.

Die Zufallsfolge wird durch eine von einem Zufallsgenerator ausgegebene Zufallszahl erzeugt. Es ist zweckmäßig, die Zufälligkeit zusätzlich zu modifizieren. Beispielsweise kann die Cache-Steuerung die Anzahl der Cache-Misses und Cache-Hits in einem vorgegebenen Zeitraum protokollieren und zusätzliche Cache-Miss-Ereignisse so einstellen, daß sich gemittelt über den Zeitraum eine Gleichverteilung von Cache-Misses und Cache-Hits entsprechend einem Vorgabewert einstellt. Hierzu werden in Abhängigkeit von dieser Statistik zusätzliche Cache-Misses erzeugt. Die Cache-Miss-Rate wird entsprechend der Statistik dynamisch nachgestellt, so daß sich im eingeschwungenen Zustand ein festes Verhältnis zwischen der Anzahl von Cache-Misses und Cache-Hits im vorgegebenen Zeitintervall einstellt. Es ist dann nicht mehr möglich, aufgrund der Abfolge von Cache-Miss- oder Cache-Hit-Ereignissen auf den Programmablauf des Mikroprozessors rückzuschließen.

Ein Cache-Miss führt zu einer hohen Arbeitsbelastung des Mikroprozessors. Die Rechenleistung des Systems sinkt dann. Es ist daher zweckmäßig, daß gerade dann Cache-Misses zusätzlich erzeugt werden, wenn die Auslastung des Mikroprozessors gering ist. Bei hoher Auslastung des Mikroprozessors wird die Cache-Miss-Rate verringert. Das Einfügen von zusätzlichen Cache-Misses wird zweckmäßigerweise abhängig von der abzuarbeitenden Software ausgeführt. Bei dieser Ausführungsform kann über die Software ein jeweils an die Applikation angepaßter Kompromiß zwischen Rechenleistung und Sicherheit eingestellt werden.

Die Erfindung wird nachfolgend anhand der in der Zeichnung dargestellten Figur näher erläutert.

- 5 Die Figur zeigt einen Mikroprozessor mit externem Speicher. Der Mikroprozessor umfaßt eine zentrale Verarbeitungseinheit (CPU) 1 und eine Cache-Einrichtung 2. CPU und Cache Einrichtung sind auf dem gleichen Halbleiterchip integriert. Die Cache-Einrichtung umfaßt das Speicherzellenfeld 21 sowie die
- 10 Cache-Steuerungseinrichtung 22. Der Mikroprozessor ist mit einem externen Speicher 3 verbunden, der auf einem weiteren Halbleiterchip realisiert sein kann oder auf dem gleichen Halbleiterchip integriert ist. Das dargestellte Mikroprozessorsystem kann beispielsweise in einer Chipkarte angeordnet
- 15 sein, die mit einem Lesegerät, beispielsweise einem Bankautomaten, kommuniziert. Der Mikroprozessor berechnet die Ver- und Entschlüsselung des Datenverkehrs zwischen Lesegerät und Chipkarte. Während des von der CPU 1 abgearbeiteten Programms werden Daten, Programmbefehle und Adressen- oder Page-
- 20 Zugriffstabellen virtueller Speichersysteme aus dem Speicher abgerufen. Diese Informationen sind im externen Speicher 3 abgelegt. Da Zugriffe auf den externen Speicher relativ lange dauern, wird ein Teil der Daten des Speichers 3 im Cache-Speicher 21 zwischengepuffert. Der Cache-Speicher 2 ist
- 25 schaltungstechnisch so ausgeführt, daß er angeforderte Daten schneller der CPU bereitstellen kann als der externe Speicher 3. Das Zusammenwirken zwischen Cache-Speicher 21 und externem Speicher 3 wird von der Cache-Steuerungseinrichtung 22, sogenannter Cache-Controller, abgewickelt.
- 30 Bei einem Lesevorgang der CPU 1 wird die Adresse ADR an den Cache-Controller 22 übermittelt. Der Cache-Controller 22 überprüft den Inhalt des Cache-Speichers 21 daraufhin, ob die angeforderte Information dort zwischengespeichert ist. Hierzu
- 35 werden die Adressen ADR an das Speicherzellenfeld 21 übermittelt. Eine Trefferlogikeinrichtung 221 stellt fest, ob das angeforderte Datum im Cache-Speicher 21 enthalten ist. Ein

Ausgangssignal HM der Trefferlogik 221 zeigt das Ergebnis dieser Feststellung an. Das Signal HM wird an die CPU 1 übertragen. Der Zustand des Signals HM zeigt der CPU 1 an, ob sich die angeforderten Daten im Cache-Speicher 21 befinden
5 oder im externen Speicher 3. Abhängig davon wird der Datenwert entweder direkt aus dem Cache-Speicher 21 geladen oder aus dem externen Speicher 3.

Wenn die Daten im Cache-Speicher 21 vorliegen (Cache-Hit),
10 werden diese über den Datenbus als Datensignal DATA an den Cache-Controller 22 übertragen, welcher sie weiter an die CPU 1 leitet. Wenn die angeforderten Daten nicht im Cache-Speicher 21 enthalten sind (Cache-Miss), erfolgt ein länger dauernder Zugriff auf den externen Speicher 3. Hierzu werden
15 die Adressen ADR an den externen Speicher 3 vom Cache-Controller 22 übertragen. Die angeforderten Daten werden zuerst an das Cache-Speicherzellenfeld 21 übertragen und dort zwischengespeichert, so daß sie bei einem nächsten Zugriff dort vorhanden sind und schneller abgefragt werden können als
20 bei einem Zugriff aus dem externen Speicher 3. Über den Cache-Controller 22 werden die Daten DATA dann an die CPU 1 weitergeleitet. Je nach dem vom Cache-Controller 22 abgearbeiteten Zugriffssteuerungsverfahren werden nicht nur die angeforderten Daten selbst, sondern auch ein geeignetes Umfeld
25 dieser Daten im Cache-Speicherzellenfeld 21 zwischengepuffert. Die Steuerung dieses Nachfüllvorgangs wird von der Fülllogikeinrichtung 222 ausgeführt.

Bei einem Cache-Miss dauert es eine gewisse Zeitspanne, bis
30 das Cache-Speicherzellenfeld 21 durchsucht worden ist und festgestellt wird, daß die angeforderten Daten nicht im Speicherzellenfeld 21 vorhanden sind. Anschließend verstreicht Zeit, bis der externe Speicher 3 zu einem Auslesen von Daten bereit ist. Während dieser Zeit ist der Stromverbrauch niedrig.
35 Danach jedoch sind eine Vielzahl von Schaltvorgängen erforderlich, um die vom externen Speicher 3 bereitgestellten Daten in den Cache-Speicher 21 einzulesen und der CPU 1 be-

reitzustellen. Der Stromverbrauch ist entsprechend hoch. Bei einem Cache-Hit stehen die angeforderten Daten relativ schnell zur Verfügung, so daß der Stromverbrauch unmittelbar nach der Anforderung hoch ist, aber nur kurze Zeit anhält.

5

Um Rückschlüsse auf den Programmablauf aufgrund des von außen meßbaren Stromverbrauchs unmöglich zu machen, werden zusätzliche Cache-Miss-Ereignisse bei einer Anfrage an den Speicher eingefügt. Auch wenn die Trefferlogik 221 feststellt, daß ein
10 Cache-Hit vorliegt, wird die Anfrage so behandelt, als ob ein Cache-Miss vorgelegen hätte. Dies bedeutet, daß ein Zugriff auf den externen Speicher 3 erfolgt und der Cache-Speicher 21 nachgeladen wird. Anstelle eines Stromprofils für den Cache-Hit ergibt sich das charakteristische Stromprofil für einen
15 Cache-Miss. Hierzu ist im Cache-Controller 22 ein Umschalter oder Multiplexer 223 vorgesehen, dessen Umschaltsignal R von einem Zufallsgenerator 224 bereitgestellt wird. Der Umschalter 223 schaltet zwischen dem Signal HM aus der Trefferlogik und einem Signal M um, welches einen Cache-Miss anzeigt. Dies
20 bedeutet, daß in Abhängigkeit von dem vom Zufallsgenerator 224 zufällsmäßig bereitgestellten Bit des Umschaltsignals R an die CPU 1 bei einem Speicherzugriff ein Cache-Miss-Ereignis übermittelt wird. Auch wenn die Trefferlogik 221 einen Cache-Hit ermittelt hat, wird der CPU 1 ein Cache-Miss
25 mitgeteilt, wenn der Umschalter 223 auf das Signal M umgeschaltet ist.

Zwischen den Zufallsgenerator 224 und den Umschalter 223 ist zweckmäßigerweise noch eine Zufallssteuerung 225 geschaltet.
30 Die Zufallssteuerung 225 modifiziert das vom Zufallsgenerator 224 erzeugte Zufallssignal in vorteilhafter Weise.

Die Zufallssteuerung 225 sorgt in einer Ausführung dafür, daß zwischen Cache-Misses und Cache-Hits innerhalb einer vorgege-
35 bener Zeitdauer eine Gleichverteilung vorliegt. Hierzu erstellt die Zufallssteuerung 225 eine Statistik, bei der die Anzahl der Cache-Miss- und Cache-Hit-Ereignisse protokolliert

wird. Es werden nun so viele zusätzliche Cache-Miss-Zugriffe eingeführt, daß innerhalb des vorgegebenen Zeitraums die Anzahl der Cache-Hits und die Anzahl der Cache-Misses je einem vorgegebenen Wert entspricht. Der für die Anzahl der Cache-Misses und Cache-Hits eingestellte Vorgabewert kann gleich
5 oder verschieden voneinander sein. Über die Betriebszeit gesehen ergibt sich nach außen hin für Cache-Misses und Cache-Hits eine Gleichverteilung. Es sind dementsprechend viele Cache-Misses zusätzlich einzufügen, daß sich der jeweilige
10 Vorgabewert für die Anzahl von Cache-Misses und Cache-Hits pro vorgegebenem Zeitintervall einstellt. Aus dem Stromprofil kann dann kein Rückschluß mehr auf den Kontrollfluß der Software/Firmware des Mikroprozessors gezogen werden. Die Einfügung zusätzlicher Cache-Misses erfolgt auch bei dieser Ausführung
15 zufallsgesteuert.

In einer anderen Ausführung bewirkt die Zufallssteuerung 225 eine von der Auslastung der CPU 1 abhängige Einfügung von zusätzlichen Cache-Misses. Hierzu wird in der CPU 1 ein Signal
20 erzeugt, welches der Zufallssteuerung 225 zugeführt wird und den momentanen Auslastungsgrad der CPU 1 angibt. Wenn die CPU 1 gering ausgelastet ist, wird die Cache-Miss-Rate, d.h. die Anzahl der notwendigen und zusätzlichen Cache-Miss-Ereignisse pro vorgegebenen Zeitintervall, angehoben. Bei hoher Auslastung
25 hingegen soll die Rechenleistung nicht weiter durch langsame Speicherzugriffe belastet werden, so daß die Cache-Miss-Rate reduziert wird. In jedem Fall erfolgt die Einfügung von zusätzlichen Cache-Miss-Ereignissen, d.h. solche, die trotz eines von der Trefferlogik 221 festgestellten Cache-Hits
30 ausgeführt werden, in zufälliger Weise gesteuert durch den Zufallsgenerator 224. Bei niedriger Cache-Miss-Rate wird die Abhörsicherheit mittels Stromprofilmessung zwar verringert, dem Mikroprozessorsystem steht aber demgegenüber ausreichend hohe Rechenleistung zur Verfügung, um die abgearbeitete Applikation auszuführen. Über die Software wird ein
35 jeweils an die Applikation angepaßter Kompromiß zwischen Rechenleistung und Sicherheit individuell konfiguriert.

Obwohl die vorgenannten Ausführungsbeispiele im Zusammenhang mit einem Lesezugriff beschrieben worden sind, kann die Erfindung ebenfalls auf einen über den Cache-Speicher abgewickelten Schreibzugriff ausgedehnt werden. Bei einem Schreiben von Daten in den externen Speicher 3 wird zuerst überprüft, ob die zu schreibenden Daten bereits im Cache-Speicher 21 vorhanden sind. Bei einem Cache-Hit braucht der Prozessor die Daten nicht gesondert an den externen Speicher 3 zu übertragen. Vielmehr übernimmt dies die Cache-Steuerung 22 unter Anwendung der im Cache-Speicher 21 gespeicherten Schreibdaten. Auch hier wird entsprechend den obigen Ausführungen an die CPU 1 anstelle eines tatsächlich vorliegenden Cache-Hits ein Cache-Miss mitgeteilt. Auch hier ist über die Zufallssteuerung 225 eine Modifikation des vom Zufallsgenerator 224 erzeugten Zufallssignals möglich. Es können bei Schreibzugriffen Cache-Misses und Cache-Hits in einem vorgegebenen Zeitraum protokolliert und entsprechend einem Vorgabewert als eine Gleichverteilung gemittelt über den Zeitraum eingestellt werden, wobei dementsprechend viele zusätzlichen Cache-Misses eingefügt werden. Andererseits ist es möglich, die Cache-Miss-Rate entsprechend der Rechenleistung des Systems bei höherer Auslastung zu erniedrigen und bei niedriger Auslastung zu erhöhen.

Patentansprüche

1. Verfahren zum Zugriff eines Mikroprozessors (1) auf einen Speicher (3), bei dem ein Cache-Speicher (21) vorgesehen ist, in dem Teile des Inhaltes des Speichers (3) zwischenspeicherbar sind, bei dem der Mikroprozessor (1) einen gespeicherten Datenwert anfordert, bei dem festgestellt wird, ob der angeforderte gespeicherte Datenwert im Cache-Speicher (21) enthalten ist, und bei dem dann, wenn der Datenwert im Cache-Speicher (21) nicht enthalten ist, der Datenwert aus dem Speicher (3) ausgelesen wird, und bei dem ein Steuersignal (R) erzeugt wird, das dann, wenn der Datenwert im Cache-Speicher (21) enthalten ist, in Abhängigkeit des Steuersignals (R) den Datenwert entweder aus dem Cache-Speicher (21) oder aus dem Speicher (3) ausliest,
dadurch gekennzeichnet,
daß das Steuersignal (R) in zufallsgesteuerter Weise erzeugt wird.
2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
daß ein Signal (HM) erzeugt wird, welches angibt, daß der Datenwert im Cache-Speicher (21) enthalten ist, daß ein Signal (M) erzeugt wird, das angibt, daß der Datenwert nicht im Cache-Speicher (21) enthalten ist, und daß zwischen diesen Signalen (HM; M) in Abhängigkeit vom Steuersignal umgeschaltet wird.
3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
daß eine erste Anzahl der Auslesevorgänge aus dem Cache-Speicher (21) und eine zweite Anzahl der Auslesevorgänge aus dem Speicher (3) in einem vorgegebenen Zeitraum ermittelt wird, und daß das Steuersignal (R) derart erzeugt wird, daß die Anzahlen jeweils im wesentlichen einem vorgegebenen Wert entsprechen.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
daß ein Signal erzeugt wird, welches ein Maß für den Ausla-
stungsgrad des Mikroprozessors (1) ist, daß eine Anzahl der
5 Auslesevorgänge aus dem Speicher in einem vorgegebenen Zei-
tintervall ermittelt wird, und daß das Steuersignal (R) der-
art erzeugt wird, daß bei durch das Signal angezeigtem höhe-
ren Auslastungsgrad die Anzahl der Auslesevorgänge aus dem
Speicher (3) niedriger ist als bei niedrigem Auslastungsgrad.

10

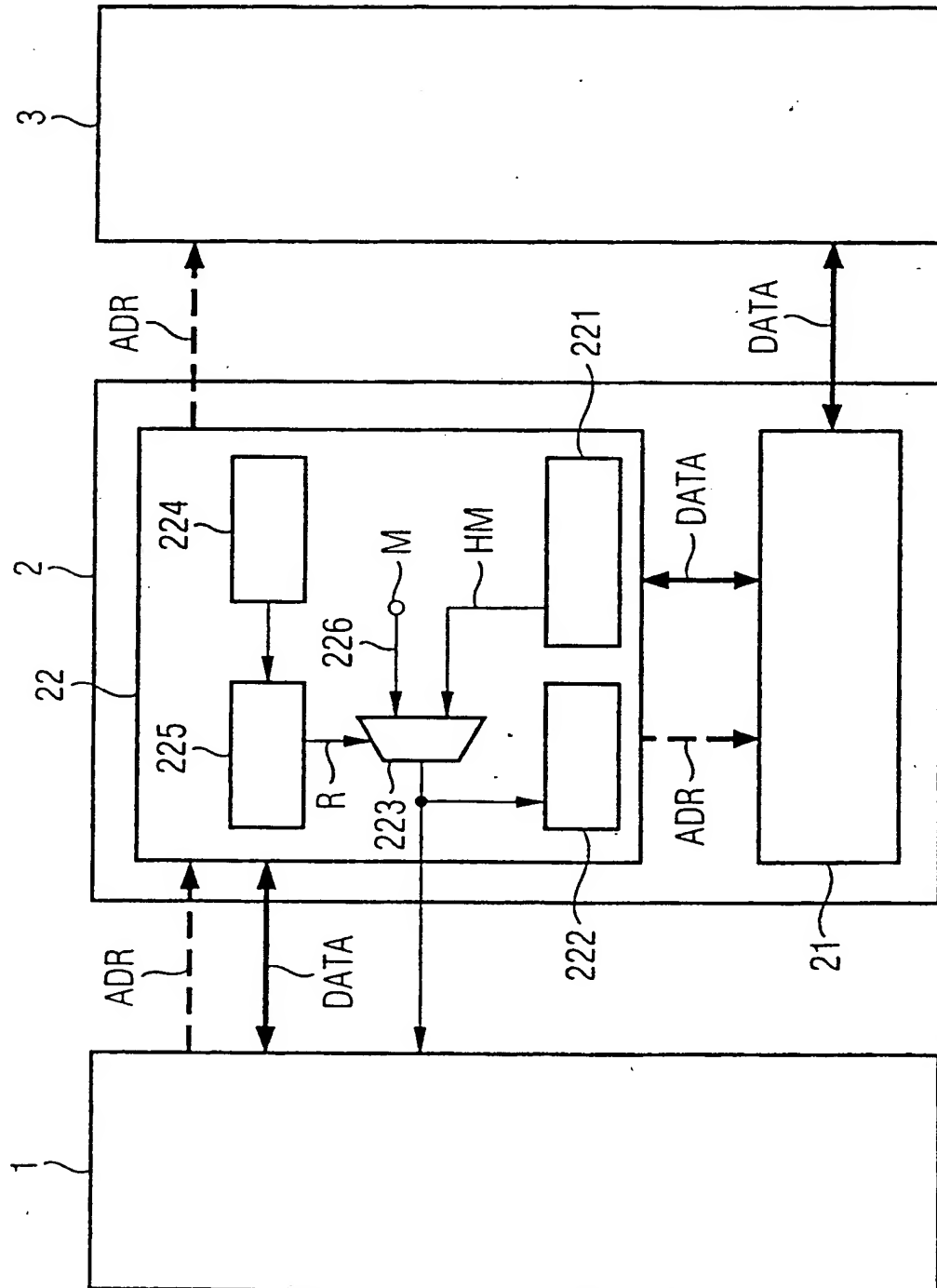
5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
daß nach dem Auslesen des Datenwertes aus dem Speicher (3)
der Datenwert in den Cache-Speicher (21) geschrieben wird.

15

6. Schaltungsanordnung zur Durchführung des Verfahrens nach
einem der Ansprüche 1 bis 5,
gekennzeichnet durch
eine zentrale Verarbeitungseinheit (1), einen Speicher (3),
20 einen Cache-Speicher (21) und eine Steuerungseinrichtung
(22), die mit der zentralen Verarbeitungseinheit (1) und dem
Cache-Speicher (21) verbunden ist, wobei die Steuerungsein-
richtung enthält: einen Zufallsgenerator (224) zur Erzeugung
eines zufallsgesteuerten Signals, eine Einrichtung zur Fest-
25 stellung (221), ob ein von der zentralen Verarbeitungseinheit
(1) angefragter Datenwert im Cache-Speicher (21) enthalten
ist oder nicht, einen Anschluß (226) zur Bereitstellung eines
Signals (M), das angibt, daß der Datenwert nicht im Cache-
Speicher (21) enthalten ist, und eine Umschalteinrichtung
30 (223), die vom Zufallsgenerator (224) steuerbar ist, und die
eingangsseitig mit dem Anschluß (226) und der Einrichtung zur
Feststellung (221) verbunden ist, und ausgangsseitig mit der
zentralen Verarbeitungseinheit (1) gekoppelt ist, um ein Aus-
lesen entweder aus dem Speicher (3) oder aus dem Cache-
35 Speicher (21) in Abhängigkeit von einem an der Umschaltein-
richtung (223) ausgangsseitig anliegenden Signal steuerbar
ist.

7. Schaltungsanordnung nach Anspruch 6,
g e k e n n z e i c h n e t d u r c h
eine weitere Steuerungseinrichtung (222), durch die ein aus
5 dem Speicher (3) ausgelesener Datenwert in den Cache-Speicher
(21) geschrieben wird, die von der Umschalteinrichtung (223)
ausgangsseitig steuerbar ist.
8. Schaltungsanordnung nach einem der Ansprüche 6 oder 7,
10 d a d u r c h g e k e n n z e i c h n e t ,
daß der Zufallsgenerator (224) eine Steuerung (225) umfaßt,
durch die das zufallsgesteuerte Signal in Abhängigkeit von
der Anzahl von Zugriffen von der zentralen Verarbeitungsein-
heit (1) auf den Speicher (3) und/oder der Anzahl der Zugrif-
15 fe der zentralen Verarbeitungseinheit (1) auf den Cache-
Speicher (21) steuerbar ist.

1/1



THIS PAGE BLANK (USPTO)

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
19. Juli 2001 (19.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/52069 A3

(51) Internationale Patentklassifikation⁷: G06F 1/00, 12/08

(21) Internationales Aktenzeichen: PCT/EP00/13134

(22) Internationales Anmeldedatum:
22. Dezember 2000 (22.12.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
00100508.1 11. Januar 2000 (11.01.2000) EP

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): INFINEON TECHNOLOGIES AG [DE/DE]; St.-
Martin-Strasse 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): GAMMEL, Berndt
[DE/DE]; Ludwig-Dill-Weg 3, 81737 München (DE).
SMOLA, Michael [DE/DE]; Julastrasse 17, 80636
München (DE).

(74) Anwalt: EPPING HERMANN & FISCHER; Postfach
12 10 26, 80034 München (DE).

(81) Bestimmungsstaaten (national): BR, CN, IN, JP, KR,
MX, RU, UA, US.

(84) Bestimmungsstaaten (regional): europäisches Patent (AT,
BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE, TR).

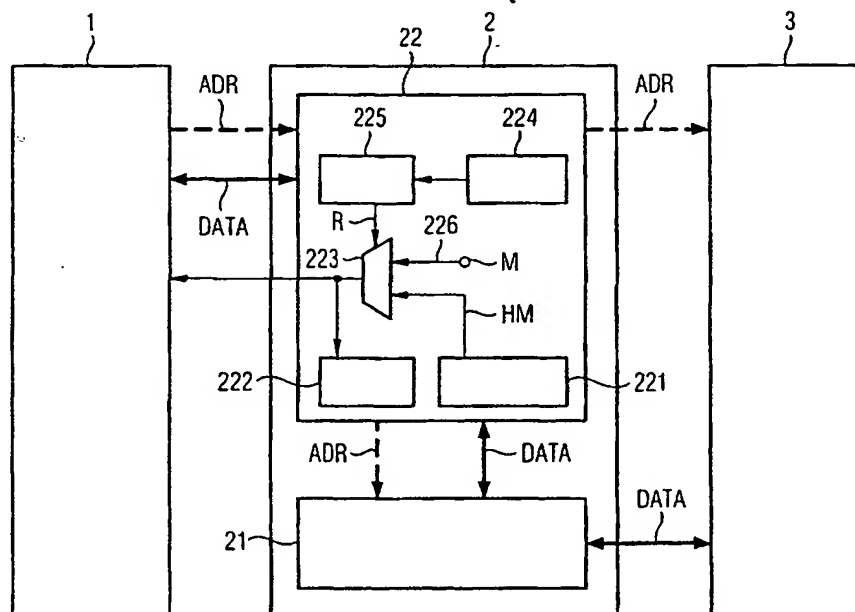
Veröffentlicht:

— mit internationalem Recherchenbericht

[Fortsetzung auf der nächsten Seite]

(54) Title: MEMORY ACCESS METHOD AND A CIRCUIT ARRANGEMENT

(54) Bezeichnung: SPEICHERZUGRIFFSVERFAHREN UND SCHALTUNGSANORDNUNG



(57) Abstract: The invention relates to a microprocessor (1). A cache memory (21) serves for accelerating access to an external memory (3). Cache miss is signalled to the microprocessor (1) instead of the actually present cache hit event. Reversal is controlled randomly. The current profile of cache hit and cache miss events is thus masked in such a way that security is increased in relation to statistic hacking methods by means of which the current profile is evaluated.

[Fortsetzung auf der nächsten Seite]



(88) Veröffentlichungsdatum des internationalen
Recherchenberichts:

21. Februar 2002

*Zur Erklärung der Zweibuchstaben-Codes und der anderen
Abkürzungen wird auf die Erklärungen ("Guidance Notes on
Codes and Abbreviations") am Anfang jeder regulären Ausgabe
der PCT-Gazette verwiesen.*

(57) Zusammenfassung: Bei einem Mikroprozessor (1) dient ein Cache-Speicher (21) zur Beschleunigung von Zugriffen auf einen externen Speicher (3). Anstelle eines tatsächlich vorliegenden Cache-Hit-Ereignisses wird dem Mikroprozessor (1) ein Cache-Miss gemeldet. Die Umsteuerung erfolgt zufallsgesteuert. Dadurch wird das Stromprofil von Cache-Hit- und Cache-Miss-Ereignissen verschleiert, so dass die Sicherheit gegenüber statistischen das Stromprofil auswertenden Angriffsverfahren erhöht wird.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/13134

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F1/00 G06F12/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 765 194 A (MCBRIDE JOHN G) 9 June 1998 (1998-06-09) column 1, line 26 -column 3, line 5 ----	1,2,5-7
A	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 June 1990 (1990-06-05) column 2, line 29 -column 3, line 5 ----	1,6
A	US 5 500 601 A (FOURNEL RICHARD ET AL) 19 March 1996 (1996-03-19) column 2, line 1 - line 47 -----	1,6

☐ Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents:

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

Z document member of the same patent family

Date of the actual completion of the international search

6 July 2001

Date of mailing of the international search report

16/07/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040. Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Nielsen, O

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/13134

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5765194	A	09-06-1998	DE 19709229 A	13-11-1997
			GB 2312768 A,B	05-11-1997
			JP 10091520 A	10-04-1998
US 4932053	A	05-06-1990	FR 2638869 A	11-05-1990
			DE 68900160 D	29-08-1991
			EP 0368727 A	16-05-1990
			JP 2199561 A	07-08-1990
			JP 2813663 B	22-10-1998
US 5500601	A	19-03-1996	FR 2673295 A	28-08-1992
			DE 69220979 D	28-08-1997
			DE 69220979 T	12-02-1998
			DE 500461 T	04-02-1993
			EP 0500461 A	26-08-1992

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F1/00 G06F12/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 765 194 A (MCBRIDE JOHN G) 9. Juni 1998 (1998-06-09) Spalte 1, Zeile 26 - Spalte 3, Zeile 5 ---	1,2,5-7
A	US 4 932 053 A (FRUHAUF SERGE ET AL) 5. Juni 1990 (1990-06-05) Spalte 2, Zeile 29 - Spalte 3, Zeile 5 ---	1,6
A	US 5 500 601 A (FOURNEL RICHARD ET AL) 19. März 1996 (1996-03-19) Spalte 2, Zeile 1 - Zeile 47 -----	1,6



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

6. Juli 2001

Absendedatum des internationalen Recherchenberichts

16/07/2001

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Nielsen, O

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 00/13134

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5765194 A	09-06-1998	DE 19709229 A	13-11-1997
		GB 2312768 A, B	05-11-1997
		JP 10091520 A	10-04-1998
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		DE 68900160 D	29-08-1991
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
US 5500601 A	19-03-1996	FR 2673295 A	28-08-1992
		DE 69220979 D	28-08-1997
		DE 69220979 T	12-02-1998
		DE 500461 T	04-02-1993
		EP 0500461 A	26-08-1992